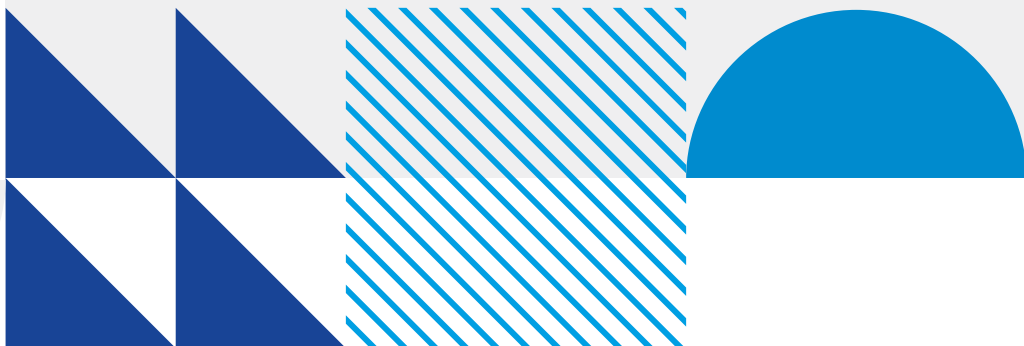

How do you stay one step ahead of phishing and cyber attacks?

THE GROWING ROLE OF CYBERCRIME



Always one step ahead of phishing and cyber attacks

As an organisation with **multiple network users**, you are always looking for the most effective way to protect that network, right?

Unfortunately, simply installing a firewall and anti-malware is no longer enough. To prevent resourceful hackers from getting a foot in the door, you need extra protection.

- The main shortcoming of standard cybersecurity solutions is that they are not fast enough in recognising and blocking **new threats**. This is because they do not detect the threat until it has already entered the network.

- This leaves your network – and in turn your business data – unprotected against threats that are only just emerging but could significantly damage your business. There is also the risk of reputational damage or your business being temporarily unavailable due to the impact of an attack on your network.

It is therefore important to always **stay one step ahead of those new dangers**. With an extra layer on top of your existing package, you minimise potential damage within your network. And that can now be done with an accessible and immediately installed solution made right here in Belgium: Secutec SecureDNS.



“We weren’t actually looking for an additional tool, because we weren’t aware of the problem. After a brief and effective test with Secutec SecureDNS, we chose to add this extra layer of security.”

Philippe Maquoi, Operational security team leader at SPW

What risks do you face despite your current cybersecurity solutions?

Cybercrime continues to rise, and phishing, a 'trick' to steal data using malware, is particularly gaining in popularity. The number of cases of ransomware, in which cybercriminals hold a company's network hostage in exchange for a ransom, also continues to rise sharply. This form of cybercrime is highly profitable for hackers, because it often involves large sums of ransom money and the risk of getting caught is small.

The best solution to secure your network against cybercrime is to have the network monitored from the outside. A hacker looks for the so-called sweet spots: the greatest external weaknesses.

As much as 91% of all malware uses unsecured DNS connections. By excluding these, you therefore also immediately close off a large part of the risks. Which is precisely what Secutec SecureDNS does: A very rapid reputation check of websites which are requested by employees.

Secutec SecureDNS thus provides an extra layer of protection. That way, you run significantly less risk:

- Costs due to an interruption of your operation due to server failure.
- Comprehensive and alarming data breaches.
- Loss of customers who lose confidence in your organisation.

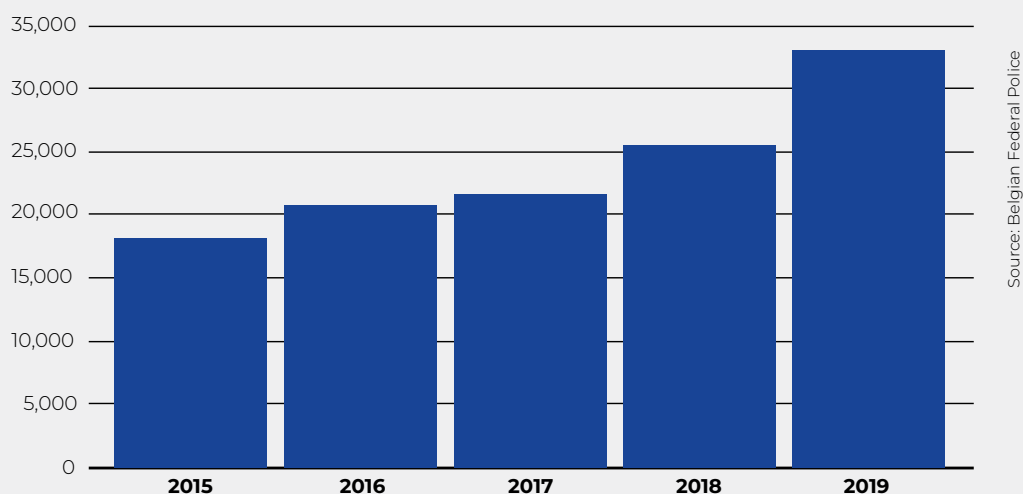


“Through Secutec Secure DNS’s weekly reporting, we saw a huge increase in phishing websites capitalising on the news around Covid-19 – all unsafe connections that Secutec SecureDNS prevented.”

Pieter Verheyden, senior system engineer at VAB

Cybersecurity today

Nearly 33,000 cases of cybercrime were reported in 2019. That represents an increase of 30% over the previous year. E-commerce has a major share in this growth. With more people ordering online, the opportunities for hackers to strike are increasing, and the growing number of employees working from home also poses a security challenge for organisations.



Most 'cyber threats' are hidden inconspicuously in seemingly trustworthy and legitimate documents, emails, apps and websites.

[Consultancy firm BDO](#) analysed 15,000 websites and concluded that one out of every five government and corporate websites in Belgium are easy targets for hackers.

According to anti-phishing platform Phished, [in 2020, as many as 22% of recipients of phishing messages were caught in the trap](#). This trend will continue, so you must actively urge your employees to be **vigilant**.

But don't count on that alone: phishers are clever, and an extra layer of protection is no mere luxury. Especially since the 'bait' used in phishing is **messages related to current events** on topics of uncertainty and importance, such as the Covid-19 vaccine.

An extra layer of protection: why is it so important?

Secutec Secure DNS's extra layer of protection secures the DNS connections your users make.



What is a DNS connection?

A **DNS** or **Domain Name Server** matches the IP address of your employee or network user to the **website name** or **URL** that the user is trying to reach either by typing it into their browser or by clicking on a link.

So a DNS is actually the '**phone book of the Internet**': a virtual collection of all users and their IP addresses.

What makes a DNS connection so vulnerable?

Unlike IP addresses, DNS connections **often remain unsecured**. Hackers with bad intentions know this too: more than 91% of all malware uses DNS to connect to your server and steal data there or redirect traffic to malicious websites.

An added layer to your current protection

To be clear: Secutec SecureDNS does not replace your current protection package, but rather adds to it. Your existing cybersecurity package is the door to your home. With Secutec SecureDNS, you turn the lock.

Secutec SecureDNS helps you do business with peace of mind by giving you insight into your organisation's digital security, without unnecessary technical details.

The main advantages of Secutec SecureDNS

- Secutec SecureDNS **blocks more threats faster** than other protection software.
- **No server reboot** or server pause is required for start up.
- Our specialist implements SecureDNS in **less than an hour** by means of an efficient remote call.
- SecureDNS works independently of system, network or security, and is therefore **accessible to everyone**.
- Do you have **remote workers** using a different network? Their traffic is also automatically redirected and controlled by means of the Secutec SecureDNS server.
- You regularly receive **detailed and personalised reports** showing what was blocked and who tried to reach suspicious sites.
- Each installation is **tailored** to the needs of your business.
- When we identify a threat, you immediately receive an **alert**.
- You feel **constantly secure** thanks to the support of our experts.
- **We keep all devices safe**, even those over which you have no control, such as educational institutions with a guest network for students.



*“Secutec SecureDNS
is ridiculously easy to implement.
It takes mere seconds.”*

Pieter Verheyden, senior system engineer at VAB



CYBERSECURITYTM
MADE IN EUROPE

Accessible and Belgian, but on an international level

Secutec is a **Belgian security specialist** that stands for high quality, quick response and lasting, professional relationships.

We protect large and international companies and organisations, but we are locally anchored in Belgium, so we can respond perfectly to your needs.

We use both local information and information from renowned international security solution providers.

You
can have
a free trial of
Secutec
SecureDNS
**for 4
weeks.**

There's no time to lose: protect your precious data from digital attacks.
Contact us at sales@secutec.be
or +32(0)3-877 82 93

